On the Throughput of Secure Hybrid-ARQ Protocols for Gaussian Block-Fading Channels

Xiaojun Tang, Ruoheng Liu, Predrag Spasojević, and H. Vincent Poor

Abstract

The focus of this paper is an information-theoretic study of retransmission protocols for reliable packet communication under a secrecy constraint. The *h*ybrid *a*utomatic *r*etransmission re*q*uest (HARQ) protocol is revisited for a block-fading wire-tap channel, in which two legitimate users communicate over a block-fading channel in the presence of a passive eavesdropper who intercepts the transmissions through an independent block-fading channel. In this model, the transmitter obtains a 1-bit ACK/NACK feedback from the legitimate receiver via an error-free *public* channel. Both reliability and confidentiality of secure HARQ protocols are studied by the joint consideration of channel coding, secrecy coding, and retransmission protocols. In particular, the error and secrecy performance of *repetition time diversity* (RTD) and *incremental redundancy* (INR) protocols are investigated based on *good* Wyner code sequences, which ensure that the confidential message is decoded successfully by the legitimate receiver and is kept in total ignorance by the eavesdropper for a given set of channel realizations. This paper first illustrates that there exists a *good* rate-compatible Wyner code family which ensures a secure INR protocol. Next, two types of outage probabilities, *connection outage* and *secrecy outage* probabilities are defined in order to characterize the tradeoff between the reliability of the legitimate communication link and the confidentiality with respect to the eavesdropper's link. For a given connection/secrecy outage probability pair, an achievable throughput of secure HARQ protocols is derived for block-fading channels. Finally, both asymptotic analysis and numerical computations demonstrate the benefits of HARQ protocols to throughput and secrecy.

This research was supported by the National Science Foundation under Grants ANI-03-38807, CNS-06-25637 and CCF-07-28208. The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Nice, France, June 24 - 29, 2007.

X. Tang and P. Spasojević are with Wireless Information Network Laboratory (WINLAB), Department of Electrical and Computer Engineering, Rutgers University, North Brunswick, NJ 08902, USA (e-mail: {xtang,spasojev}@winlab.rutgers.edu).

R. Liu and H. V. Poor are with Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA (email: {rliu,poor}@princeton.edu).

Index Terms

Information-theoretic secrecy, HARQ, block-fading, rate compatible punctured codes, incremental redundancy, time diversity.

I. Introduction

Reliable communication is essential in applications of wireless packet-oriented data networks. A class of special coding schemes, the so-called hybrid automatic retransmission request (HARQ), combine powerful channel coding with retransmission protocols to enhance the reliability of communication links. Among currently available HARQ protocols, the most elementary form is the *repetition-coding-based* HARQ which combines several noisy observations of the same packet by using a suitable diversity technique at the receiver, such as maximal-ratio combining, equal-gain combining, or selection combining. A more powerful HARQ scheme is the so-called *incremental redundancy* HARQ, which achieves higher throughput efficiency by adapting its error correcting code redundancy to fluctuating channel conditions. In an incremental redundancy scheme, the message is encoded at the transmitter by a "mother" code. Initially, only a selected number of coded symbols are transmitted. The selected number of coded symbols form a codeword of a punctured mother code. If a retransmission is requested, additional redundancy symbols are sent under possibly different channel conditions. An information-theoretic analysis of the throughput performance of HARQ protocols over block-fading Gaussian collision channels is found in [1]. By assuming Gaussian random coding and typical-set decoding, the results of [1] are independent of the particular coding/decoding technique and can be regarded as providing a limiting performance in the information-theoretic sense. Another line of recent research on HARQ concerned with various mother codes and their puncturing can be found in [2]–[8].

Confidentiality is a basic requirement for secure communication over wireless networks. We note that the broadcast nature of the wireless medium gives rise to a number of security issues. In particular, wireless transmission is very susceptible to eavesdropping since anyone within communication range can listen to the traffic and possibly extract information. Traditionally, confidentiality has been provided by using cryptographic methods, which rely heavily on secret keys. However, the distribution and maintenance of secret keys are still open issues for large wireless networks. Fortunately, confidential communication is possible without sharing a secret key between legitimate users. This was shown by Wyner in his seminal paper [9]. In the discrete memoryless wire-tap channel model he proposed, the communication between two legitimate users is eavesdropped upon via a degraded channel (the eavesdropper channel). The level

of ignorance of the eavesdropper with respect to the confidential message is measured by the equivocation rate. Perfect secrecy requires that the equivocation rate should be asymptotically equal to the message entropy rate. Wyner showed that perfect secrecy can be achieved via a stochastic code, referred to as Wyner secrecy code. Csiszár and Körner generalized this result and determined the secrecy capacity region of the broadcast channel with confidential messages in [10]. Recent research investigates multi-user communication with confidential messages, e.g., multiple access channels with confidential messages [11], [12], multiple access wire-tap channels [13], and interference channels with confidential messages [14]. The effect of fading on secure communication has been studied in [15]–[18]. More specifically, assuming that all communicating parties have perfect channel state information (CSI) prior to the message transmission, [15] has studied the delay limited secrecy capacity of wireless channels, while [16]–[18] have studied the secrecy capacity of an ergodic fading channel. [18] has also considered the ergodic scenario in which the transmitter has no CSI about the eavesdropper channel.

In this paper, we investigate secure packet communication based on HARQ protocols. The challenge of this problem is twofold: first, the encoder at the transmitter needs to provide sufficient redundancy for the legitimate receiver to decode its message successfully; on the other hand, too much redundancy may help adversarial eavesdropping. As an example, retransmission is an effective way to enhance reliability, but nevertheless it may also compromise confidentiality. This motivates the joint consideration of channel coding, secrecy coding, and retransmission protocols.

We consider a frequency-flat block-fading Gaussian wire-tap channel. In this model, a transmitter sends confidential messages to a legitimate receiver via a block-fading channel in the presence of a passive eavesdropper who intercepts the transmission through an independent block-fading channel. We assume that the transmitter has no perfect CSI, but receives a 1-bit ACK/NACK feedback from the legitimate receiver via a reliable public channel. Under this setting, we study the secure HARQ protocols from an information theoretic point of view. In particular, the error and secrecy performance of *repetition time diversity* (RTD) and *incremental redundancy* (INR) protocols are investigated based on *good* Wyner code sequences, which ensure that the confidential message is decoded successfully by the legitimate receiver and is kept completely secret from the eavesdropper for a given set of channel realizations of both the main and the eavesdropper channels. Next, we show that there exists a *good* rate-compatible Wyner code family which suits the secure INR protocol. Due to the absence of CSI, the transmitter cannot adapt its code and power level to channel conditions. Instead, for a given mother code, we consider the outage performance of secure HARQ protocols. Specifically, we define two types of outage: *connection outage* and *secrecy outage*. The outage probabilities (i.e., the probabilities of connection and secrecy

outage) are used to characterize the tradeoff between the reliability of the legitimate communication link and the confidentiality with respect to the eavesdropper's link. We evaluate the achievable throughput of HARQ protocols under the constraints on these two outage probabilities. Finally, we compare the secrecy throughput of two HARQ protocols through both numerical computations and an asymptotic analysis, and illustrate the benefit of HARQ schemes to information secrecy.

Generally speaking, when the coding parameters (main channel code rate and secrecy information rate for ensuring reliability and secrecy, respectively) can be freely chosen, INR can achieve a significantly larger throughput than RTD, which concurs with the results not involving secrecy where it has been shown that mutual-information accumulation (INR) is a more effective approach than SNR-accumulation (RTD) [1]. However, when one is forced to ensure small connection outage for the main channel even when it is bad, one is forced to reduce the main channel code rate. The INR scheme, having a larger coding gain (to both the intended receiver and the eavesdropper), needs to sacrifice a larger portion of the main channel code rate in order to satisfy the secrecy requirement. Hence, when the main channel code rate is bounded due to the connection outage constraint, the achievable secrecy throughput of INR may be smaller than that of RTD. This result deviates from that not involving secrecy.

The remainder of this paper is organized as follows. We describe the system model and preliminaries in Section II. In Section III, we prove the existence of good Wyner codes for parallel channel communication and define outage events, while these results are applied to INR and RTD protocols in Section IV. We derive the secrecy throughput of two protocols over block fading channels in Section V, and present an asymptotic analysis in Section VI. We illustrate and compare the various results and protocols numerically in Section VII. Finally, we give conclusions and some interesting directions for future research in Section VIII, The proofs of the results are provided in appendices.

II. System Model and Preliminaries

A. System Model

As shown in Fig. 1, we consider a model in which a transmitter sends confidential messages to a destination via a source-destination channel (the main channel) in the presence of a passive eavesdropper which listens to the transmission through a source-eavesdropper channel (the eavesdropper channel). Both the main channel and the eavesdropper channel experience M-block fading, in which the channel gain is constant within a block while varying independently from block to block [19], [20]. We assume that each block is associated with a time slot of duration T and bandwidth W; that is, the transmitter can

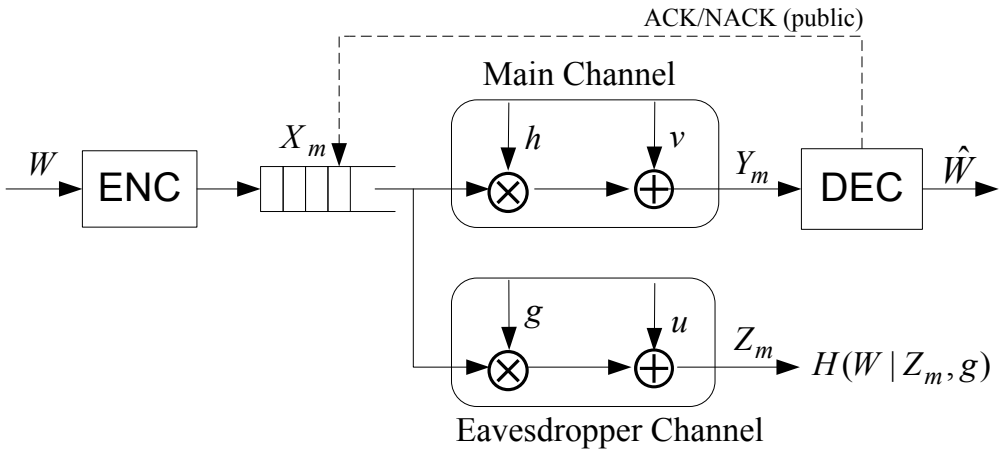

Fig. 1. System model: hybrid ARQ protocols for the block-fading channel in the presence of a passive eavesdropper

send $N = \lfloor 2WT \rfloor$ real symbols in each slot. Additionally, we assume that the number of channel uses within each slot (i.e., N) is large enough to allow for invoking random coding arguments.[1]

At the transmitter, a confidential message $w \in \mathcal{W}$ is encoded into a codeword x^{MN}, which is then divided into M blocks $[x_1^N, x_2^N, \ldots, x_M^N]$, each of length N. The codeword x^{MN} occupies M slots; that is, for $i = 1, \ldots, M$, the i-th block x_i^N is sent in slot i and received by the legitimate receiver through the channel gain h_i and by the eavesdropper through the channel gain g_i. A discrete time baseband-equivalent block-fading wire-tap channel model can be expressed as follows:

$$\begin{aligned} & y(t) = \sqrt{h_i}x(t) + v(t) \\ \text{and} \qquad & z(t) = \sqrt{g_i}x(t) + u(t) \quad \text{for } t = 1, \ldots, MN,\ i = \lceil t/N \rceil, \end{aligned} \tag{1}$$

where $x(t)$ denotes the input signal, $y(t)$ and $z(t)$ denote the output signals at the legitimate receiver and the eavesdropper, respectively, at time t ($t = 1, \ldots, MN$), $\{v(t)\}$ and $\{u(t)\}$ are independent and identically distributed (i.i.d.) $\mathcal{N}(0, 1)$ random variable sequences, and h_i and g_i, for $i = 1, \ldots, M$, denote the normalized (real) channel gains of the main channel and the eavesdropper channel, respectively. Furthermore, we assume that the signal $x(t)$ has constant average energy per symbol

$$E[|x(t)|^2] \leq \bar{P}. \tag{2}$$

[1]For example, in a 64 kb/s down-link reference data channel for universal mobile telecommunications system (UMTS) data-transmission modes, each slot can contain up to $N \approx 10000$ dimensions [21].

Let $\mathbf{h} = [h_1, \ldots, h_M]$ and $\mathbf{g} = [g_1, \ldots, g_M]$ denote vectors whose elements are the main channel gains and the eavesdropper channel gains, respectively. We refer to $(\mathbf{h}, \mathbf{g})$ as a *channel pair* and assume that the legitimate receiver knows its channel $\mathbf{h}$, while the eavesdropper knows its channel $\mathbf{g}$.

B. Wyner Codes

In this subsection, we consider a single-block transmission, i.e., $M = 1$ and introduce Wyner codes [9], which are the basis of our secure HARQ protocols.

Let $C(R_0, R_s, N)$ denote a Wyner code of size 2^{NR_0} to convey a confidential message set $\mathcal{W} = \{1, 2, \ldots, 2^{NR_s}\}$, where $R_0 \geq R_s$ and N is the codeword length. The basic idea of Wyner codes is to use a stochastic encoder to increase the secrecy level [9], [10]. Hence, there are two rate parameters associated with the Wyner code: the main channel code rate R_0 and the secrecy information rate R_s.[2] The Wyner code $C(R_0, R_s, N)$ is constructed based on random binning [9] as follows. We generate 2^{NR_0} codewords $x^N(w, v)$, where $w = 1, 2, \ldots, 2^{NR_s}$, and $v = 1, 2, \ldots, 2^{N(R_0 - R_s)}$, by choosing the $N2^{NR_0}$ symbols $x_i(w, v)$ independently at random according to the input distribution $p(x)$. A Wyner code ensemble $\mathcal{C}(R_0, R_s, N)$ is the *set* of all possible Wyner codes of length N, each corresponding to a specific generation and a specific labeling.

The stochastic encoder of $C(R_0, R_s, N)$ is described by a matrix of conditional probabilities so that, given $w \in \mathcal{W}$, we randomly and uniformly select v from $\{1, 2, \ldots, 2^{N(R_0 - R_s)}\}$ and transmit $x^N = x^N(w, v)$. We assume that the legitimate receiver employs a typical-set decoder. Given y^N, the legitimate receiver tries to find a pair $(\tilde{w}, \tilde{v})$ so that $x^N(\tilde{w}, \tilde{v})$ and y^N are jointly typical [22], i.e.,

$$\{x^N(\tilde{w}, \tilde{v}), y^N\} \in T_\epsilon^N(P_{XY}).$$

If there is no such jointly typical pair, then the decoder claims failure.

Assume that signals y^N and z^N are received at the legitimate receiver and the eavesdropper, respectively, via a channel pair (h, g). The average error probability is defined as

$$P_e(h) = \sum_{w \in \mathcal{W}} \Pr\left\{\phi\big(Y^N(w)\big) \neq w | h, w \text{ sent}\right\} \Pr(w), \tag{3}$$

where $\phi\big(Y^N(w)\big)$ is the output of the decoder at the legitimate receiver and $\Pr(w)$ is the prior probability that message $w \in \mathcal{W}$ is sent.

[2]We call $R_0 - R_s$ the secrecy gap as the rate sacrificed to ensure the secrecy requirement.

The secrecy level, i.e., the degree to which the eavesdropper is confused, is measured by the equivocation rate at the eavesdropper. *Perfect secrecy* is achieved if for all $\epsilon > 0$ the equivocation rate satisfies

$$\frac{1}{N}H(W|g, Z^N) \geq \frac{1}{N}H(W) - \epsilon. \tag{4}$$

For conciseness, we say that a code C of length N is *good* for a wire-tap channel with the channel pair (h, g) if $P_e(h) \leq \epsilon$ and the perfect secrecy requirement (4) can be achieved, for all $\epsilon > 0$ and sufficiently large N.

C. Secure HARQ Protocols

We first consider a general (in M) secure HARQ protocol for a block-fading wire-tap channel. The transmitter encodes the confidential information (and cyclic redundancy check (CRC) bits) by using a mother code of length MN. The obtained codeword x^{MN} is partitioned into M blocks represented as $[x_1^N, x_2^N, \ldots, x_M^N]$. At the first transmission, the transmitter sends the block x_1^N under the channel gain pair (h_1, g_1). Decoding of this code is performed at the intended receiver, while the secrecy level is measured at the eavesdropper. If no error is detected, the receiver sends back an acknowledgement (ACK) to stop the transmission; otherwise a negative acknowledgement (NACK) is sent to request retransmission, and the transmitter sends the block x_2^N under the channel gain pair (h_2, g_2). Now, decoding and equivocation calculation are attempted at the receiver and eavesdropper by combining the previous block x_1^N with the new block x_2^N. The procedure is repeated after each subsequent retransmission until all M blocks of the mother code are transmitted or an HARQ session completes due to the successful decoding at the intended receiver.

Now, we focus on the error performance and secrecy level after m transmissions, $m = 1, 2, \ldots, M$. Let

$$\mathbf{x}(m) = [x_1^N, \ldots, x_m^N], \quad \mathbf{y}(m) = [y_1^N, \ldots, y_m^N], \quad \text{and} \quad \mathbf{z}(m) = [z_1^N, \ldots, z_m^N]$$

denote the input, the output at the intended receiver, and the output at the eavesdropper after m transmissions, respectively. For a given channel pair $(\mathbf{h}, \mathbf{g})$, the average error probability after the m transmissions is defined as

$$P_e(m|\mathbf{h}) = \sum_{w \in \mathcal{W}} \Pr\left\{\phi\big(\mathbf{Y}_m(w)\big) \neq w | w \text{ sent}, \mathbf{h}\right\} \Pr(w), \tag{5}$$

where $\phi\big(\mathbf{Y}_m(w)\big)$ denotes the output of the decoder at the legitimate receiver after m transmissions.

The secrecy level after m transmissions is given by

$$\frac{1}{mN}H(W|\mathbf{Z}_m, \mathbf{g}).$$

We say that perfect secrecy is achieved after m transmissions if, for all $\epsilon > 0$, the equivocation rate satisfies

$$\frac{1}{mN}H(W|\mathbf{Z}_m, \mathbf{g}) \geq \frac{1}{mN}H(W) - \epsilon. \tag{6}$$

We note that this definition implies that the perfect secrecy can also be achieved after j transmissions, for $j = 1, \ldots, m-1$.

Similar to the definition of good codes for a single-block transmission, we say that a code C of length mN is *good* for the m-block transmission and a channel pair $(\mathbf{h}, \mathbf{g})$ if $P_e(m|\mathbf{h}) \leq \epsilon$ and the perfect secrecy requirement (6) can be achieved, for all $\epsilon > 0$ and sufficiently large N.

In particular, we consider the following two secure HARQ protocols based on different mother codes and different combination techniques.

1) Incremental Redundancy: In the INR secure HARQ protocol, the mother code is a Wyner code of length MN, i.e.,

$$C \in \mathcal{C}(R_0, R_s, MN).$$

In the first transmission, the transmitted coded symbols $\mathbf{x}(1) = [x_1^N]$ form a codeword of a punctured Wyner code of length N,

$$C_1 \in \mathcal{C}\left(MR_0, MR_s, N\right).$$

Similarly, after m transmission, $m = 1, \ldots, M$, the (all) transmitted coded symbols $\mathbf{x}(m) = [x_1^N, \ldots, x_m^N]$ form a codeword of a punctured Wyner code of length mN,

$$C_m \in \mathcal{C}\left(\frac{MR_0}{m}, \frac{MR_s}{m}, mN\right).$$

At the legitimate receiver and the eavesdropper, decoding and equivocation calculation are attempted, respectively, based on the punctured code C_m.

We note that the punctured codes $\{C_M, C_{M-1}, \ldots, C_1\}$ form a family of *rate-compatible* Wyner codes with the secrecy rates

$$\left\{R_s, \frac{M}{M-1}R_s, \ldots, MR_s\right\}.$$

Hence, we refer to this protocol as the INR protocol based on rate-compatible Wyner codes.

2) Repetition Time Diversity: We also consider a simple time-diversity HARQ protocol based on the repetition of a Wyner code. In this case, the mother code C is a concatenated code consisting of the Wyner code $C_1 \in \mathcal{C}\left(MR_0, MR_s, N\right)$ as the outer code and a simple repetition code of length M as the inner code, i.e.,

$$C = [\underbrace{C_1, C_1, \ldots, C_1}_{M}]. \tag{7}$$

After each transmission, decoding and equivocation calculation are performed at the receiver and the eavesdropper, respectively, based on maximal-ratio packet combining.

III. Secure Channel Set and Outage Events

In this section, we study the error performance and the secrecy level when a mother Wyner code is transmitted over M parallel channels. Results given in this section form the basis for the performance analysis of secure HARQ protocols.

For a given Wyner code, an important practical question is: under what channel conditions will the communication be reliable and secure? In the following theorem, we describe a *secure channel set* and demonstrate that there exists a Wyner code sequence good for all channel pairs in this set.

Theorem 1. *Let $\mathcal{P}$ denote the union of all channel pairs $(\mathbf{h}, \mathbf{g})$ satisfying*

$$\frac{1}{M}\sum_{i=1}^{M} I(X;Y|h_i) \geq R_0 \tag{8}$$

and

$$\frac{1}{M}\sum_{i=1}^{M} I(X;Z|g_i) \leq R_0 - R_s, \tag{9}$$

where $I(X;Y|h_i)$ and $I(X;Z|g_i)$ are single letter mutual information characterizations of the channel (1). There exists a Wyner code $C \in \mathcal{C}(R_0, R_s, MN)$ good for all channel pairs $(\mathbf{h}, \mathbf{g}) \in \mathcal{P}$.

Proof: A proof of Theorem 1 is provided in Appendix A. ■

In the system model described in Section II, the transmitter does not have any channel state information; that is, one cannot choose the code based on a particular fading channel state. Hence, it is important to show that there exists a Wyner code sequence good for all channel pairs in the secure channel set $\mathcal{P}$.

To facilitate the formulation of outage-based throughput, we define that an outage event occurs when the channel pair does not belong to the secure channel set, i.e., $(\mathbf{h}, \mathbf{g}) \notin \mathcal{P}$. Specifically, we distinguish two types of outage: *connection outage* [3] and *secrecy outage*. In particular, we say that a connection outage occurs if

$$\frac{1}{M}\sum_{i=1}^{M} I(X;Y|h_i) < R_0, \tag{10}$$

[3]The main channel is viewed as a communication link. The link is connected if a packet can be delivered to the intended receiver successfully within the delay constraint (within M transmissions), otherwise it is in the connection outage. The connection outage probability defined in this paper is also referred to as *information outage probability* in [19].

while we say that a secrecy outage occurs if

$$\frac{1}{M}\sum_{i=1}^{M} I(X;Y|g_i) > R_0 - R_s. \tag{11}$$

Accordingly, we can evaluate both connection outage and secrecy outage probabilities, which are the probabilities of each of the outage events averaged over all possible fading states. In fact, the connection outage probability can be interpreted as the limiting error probability for large block length packets; the secrecy outage probability can be regarded as an upper bound on the probability of unsecured packets. Moreover, Theorem 1 implies that the connection outage probability and the secrecy outage probability are not just average probabilities over a code ensemble, but they can be achieved by a deterministic code sequence.

IV. Secure HARQ with Wyner Codes

In this section, we evaluate the error performance and measure the secrecy level during secure HARQ sessions.

A key part of an ARQ protocol is that decoding errors should be detected, so that ACKs or NACKs can be generated accurately. A *complete decoding function* (e.g. maximum a posteriori probability decoding or maximum-likelihood decoding) requires the encoder to add extra redundancy to the information bits, which decreases the throughput slightly. The authors of [1] have shown that error detection can be accomplished by using the built-in error detection capability of suboptimal decoders.

Lemma 1. *[1, Lemma 3] For all $\epsilon > 0$ and channel $\mathbf{h}$, any code C of length MN satisfies*

$$\Pr\left(\text{undetected error}|\mathbf{h}, C\right) < \epsilon,$$

for all sufficiently large N.

Proof: The proof follows similarly to that given in [1]. ■

A. Incremental Redundancy

To evaluate the performance of the INR protocol, we employ the following M-parallel channel model. Let us focus on the decoding after m transmissions, i.e., the coded blocks $\mathbf{x}(m) = [x_1^N, \ldots, x_m^N]$ are transmitted, $m = 1, \ldots, M$. As shown in Fig. 2, the block x_i^N experiences channel pair (h_i, g_i), $i = 1, \ldots, m$. We assume that each of the punctured blocks $[x_{m+1}^N, \ldots, x_M^N]$ is sent to a dummy memoryless component channel whose output is independent of the input.

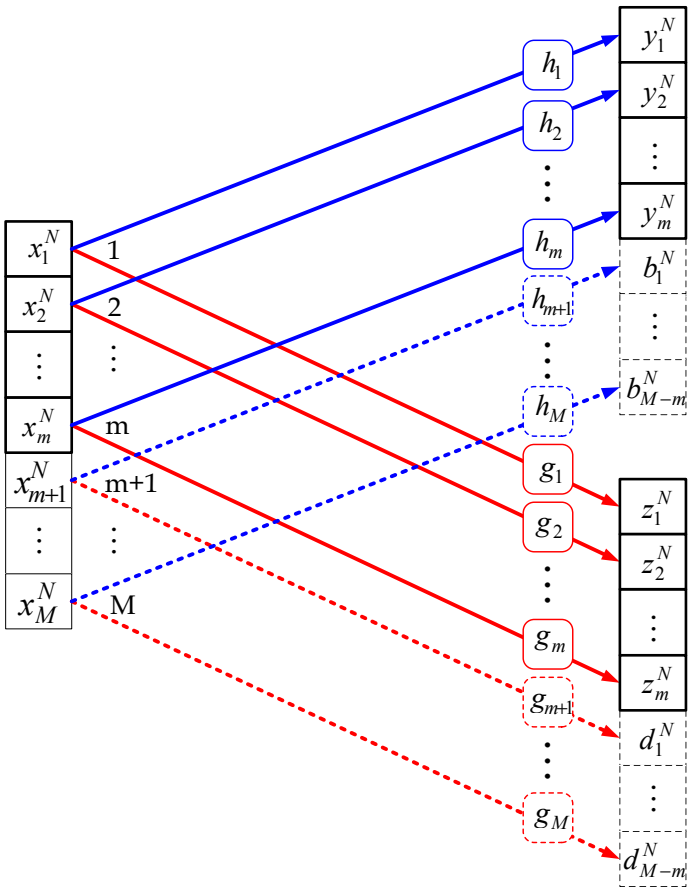

Fig. 2. M-parallel channel model for the INR protocol: the first m punctured blocks are actually transmitted (solid lines); the remaining $M-m$ punctured blocks are assumed to be sent via $M-m$ dummy memoryless channels whose outputs are independent of the inputs (dashed lines).

In this case, the mother codeword is transmitted over M parallel channels. At the legitimate receiver, the decoder combines the real signal $\mathbf{y}(m) = [y_1^N, \ldots, y_m^N]$ with $M-m$ dummy signal blocks $[b_1^N, \ldots, b_{M-m}^N]$ to form

$$[y_1^N, \ldots, y_m^N, b_1^N, \ldots, b_{M-m}^N].$$

Similarly, the processed symbols at the eavesdropper are

$$[z_1^N, \ldots, z_m^N, d_1^N, \ldots, d_{M-m}^N],$$

where $[d_1^N, \ldots, d_{M-m}^N]$ are $M-m$ dummy signal blocks. We note that the added dummy blocks do not affect either the decoding at the legitimated receiver or the equivocation calculation at the eavesdropper

since they are independent of the confidential message.

The codewords of the mother Wyner code C are transmitted in at most M transmissions during the secure HARQ session. By using the equivalent parallel channel model, we can describe this secure HARQ problem as communication over M parallel wire-tap channels and, hence, establish the following theorem.

Theorem 2. *Consider the secure INR protocol based on rate compatible Wyner codes*

$$\{C_M, C_{M-1}, \ldots, C_1\},$$

where

$$C_m \in \mathcal{C}\left(\frac{MR_0}{m}, \frac{MR_s}{m}, mN\right), \quad m = 1, \ldots, M.$$

Let $\mathcal{P}(m)$ denote the union of all channel pairs $(\mathbf{h}, \mathbf{g})$ satisfying

$$\frac{1}{M}\sum_{i=1}^{m} I(X; Y|h_i) \geq R_0, \tag{12}$$

and

$$\frac{1}{M}\sum_{i=1}^{m} I(X; Z|g_i) \leq R_0 - R_s. \tag{13}$$

Then, there exists a family of rate compatible Wyner codes $\{C_M, C_{M-1}, \ldots, C_1\}$ such that C_m is good for all channel pairs $(\mathbf{h}, \mathbf{g}) \in \mathcal{P}(m)$, for $i = 1, \ldots, M$.

Proof: We provide a proof of Theorem 2 in Appendix B. ■

B. Repetition Time Diversity

In the RTD secure HARQ protocol, both the legitimate receiver and the eavesdropper combine several noisy observations of the same packet based on diversity techniques. The optimal receivers perform maximal-ratio combining (MRC), which essentially transforms the vector channel pair $(\mathbf{h}, \mathbf{g})$ into a scalar channel pair $(\hat{h}(m), \hat{g}(m))$. Hence, after m transmissions, the equivalent channel model can be written as follows:

$$y(t) = \sqrt{\hat{h}(m)}x(t) + v(t) \quad \text{and} \quad z(t) = \sqrt{\hat{g}(m)}x(t) + u(t) \tag{14}$$

for $t = 1, \ldots, N$, where $\hat{h}(m) = \sum_{i=1}^{m} h_i$ and $\hat{g}(m) = \sum_{i=1}^{m} g_i$.

Let $\mathcal{L}(m)$ denote the union of all channel pairs $(\mathbf{h}, \mathbf{g})$ satisfying

$$I(X; Y|\hat{h}(m)) \geq MR_0, \tag{15}$$

and

$$I(X; Z|\hat{g}(m)) \leq M(R_0 - R_s), \tag{16}$$

where $I(X;Y|\hat{h}(m))$ and $I(X;Z|\hat{g}(m))$ are single letter mutual information characterizations of the channel (14). For a given (finite) M, we have the following result for the RTD secure HARQ protocol.

Corollary 1. *There exists a Wyner code* $C_1 \in \mathcal{C}\left(MR_0, MR_s, N\right)$ *such that its* m*-repeating code*

$$C_m = [\underbrace{C_1, C_1, \ldots, C_1}_{m}]$$

is good for all channel pairs $(\mathbf{h}, \mathbf{g}) \in \mathcal{L}(m)$*, for* $m = 1, \ldots, M$.

Proof: The proof follows directly from Theorem 1 by setting $M = 1$. ■

V. Secrecy Throughput of HARQ Protocols

In this section, we study the achievable secrecy throughput for HARQ protocols. We focus on Rayleigh independent block fading channels for illustration; other types of block fading channels can be studied in a similar way.

We note that the optimal input distribution of the channel (1) is not known in general when the transmitter has no CSI. For the sake of mathematical tractability, we consider Gaussian inputs. For INR, the mutual information $I_{XY}^{[\mathrm{INR}]}(m)$ and $I_{XZ}^{[\mathrm{INR}]}(m)$ can be written as

$$I_{XY}^{[\mathrm{INR}]}(m) = \frac{1}{2M}\sum_{i=1}^{m}\log_2\left(1+\lambda_i\right)$$

$$\text{and} \qquad I_{XZ}^{[\mathrm{INR}]}(m) = \frac{1}{2M}\sum_{i=1}^{m}\log_2\left(1+\nu_i\right), \tag{17}$$

where

$$\lambda_i = h_i\bar{P} \quad \text{and} \quad \nu_i = g_i\bar{P}, \quad i = 1, \ldots, M, \tag{18}$$

are the signal-to-noise ratios (SNRs) at the legitimate receiver and the eavesdropper, respectively, during transmission i. For RTD, we can express the mutual information quantities $I_{XY}^{[\mathrm{RTD}]}(m)$ and $I_{XZ}^{[\mathrm{RTD}]}(m)$ as

$$I_{XY}^{[\mathrm{RTD}]}(m) = \frac{1}{2M}\log_2\left(1+\sum_{i=1}^{m}\lambda_i\right)$$

$$\text{and} \qquad I_{XZ}^{[\mathrm{RTD}]}(m) = \frac{1}{2M}\log_2\left(1+\sum_{i=1}^{m}\nu_i\right). \tag{19}$$

Although we consider only Gaussian signaling here, the results in Section IV can be applied to other input distributions, for example, discrete signaling under modulation constraints.

Let $\mathcal{M}$ denote the number of transmissions within a HARQ session. Given a distribution of the main channel SNR λ, for both INR and RTD protocols, the probability mass function of $\mathcal{M}$ can be expressed as

$$\begin{aligned} p[\mathcal{M}=m] &= \Pr\left\{I_{XY}(m-1) < R_0 \text{ and } I_{XY}(m) \geq R_0\right\} \\ &= \Pr\left\{I_{XY}(m-1) < R_0\right\} - \Pr\left\{I_{XY}(m) < R_0\right\}, \quad m = 1, \ldots, M-1, \\ \text{and} \quad p[\mathcal{M}=M] &= \Pr\left\{I_{XY}(M-1) < R_0\right\}, \end{aligned} \tag{20}$$

where $I_{XY}(m)$ and $I_{XZ}(m)$ are chosen either from (19) or from (17) corresponding to a specific HARQ protocol. Let P_e denote the connection outage probability, and P_s denote the secrecy outage probability. The definition in (20) implies that P_e and P_s can be written as follows:

$$P_e = \Pr\left\{I_{XY}(M) < R_0\right\}, \tag{21}$$

$$\text{and} \qquad P_s = \sum_{m=1}^{M} p[m] \Pr\left\{I_{XZ}(m) > R_0 - R_s\right\}. \tag{22}$$

Now, we study the secrecy throughput based on P_e and P_s. We first consider a target secrecy outage probability ξ_s; that is, at least a fraction $1-\xi_s$ of the confidential message bits sent by the transmitter are kept completely secret. Under this constraint, the secrecy throughput η, measured in bits per second per hertz, is defined to be the average number of bits decoded at the legitimate receiver,

$$\eta = \lim_{t\to\infty} \frac{a(t)}{tN}, \tag{23}$$

where again N is the number of symbols in each block and $a(t)$ is the number of information bits successfully decoded by the intended receiver up to time slot t (when a total of tN blocks are sent). The event that the transmitter stops sending the current codeword is recognized to be a *recurrent event* [23]. A random *reward* $\mathcal{R}$ is associated with the occurrence of the recurrent event. In particular, $\mathcal{R} = MR_s$ bits/symbol if transmission stops because of successful decoding, and $\mathcal{R} = 0$ bits/symbol if it stops because successful decoding has not occurred after M transmissions. By applying the renewal-reward theorem [1], [23], we obtain the secrecy throughput as

$$\eta(R_0, R_s) = \frac{\mathbb{E}[\mathcal{R}]}{\mathbb{E}[\mathcal{M}]} = \frac{MR_s}{\mathbb{E}[\mathcal{M}]}(1-P_e), \tag{24}$$

where $\mathbb{E}[\mathcal{M}]$ is the expected number of transmissions in order to complete a codeword transmission, i.e.,

$$\begin{aligned} \mathbb{E}[\mathcal{M}] &= \sum_{m=1}^{M} m p[\mathcal{M}=m] \\ &= 1 + \sum_{m=1}^{M} \Pr\left\{I_{XY}(m) < R_0\right\}. \end{aligned} \tag{25}$$

We can properly choose the mother code parameters (R_0 and R_s) to obtain the maximum throughput while satisfying ξ_s-secrecy requirement. Hence, we consider the following problem

$$\begin{aligned} \max_{R_0,R_s} \quad & \eta(R_0,R_s) \\ \text{s.t.} \quad & P_s \leq \xi_s. \end{aligned} \tag{26}$$

The optimization problem (26) imposes a probabilistic service requirement in terms of confidentiality; that is, the service quality is acceptable as long as the probability of the secrecy outage is less than ξ_s, a parameter indicating the outage tolerance of the application. Note that P_s is a decreasing function of R_s, and η is linearly proportional to R_s. Hence, we can solve the optimization problem (26) in the following two steps: first, for given M, R_0, and ξ_s, we find the maximum value $R_s^*(R_0)$; next, we obtain the optimum R_0^*, which maximizes the secrecy throughput $\eta(R_0, R_s^*(R_0))$.

On the other hand, reliability is another important quality of service parameter. To achieve both the connection outage target ξ_e and the secrecy outage target ξ_s, we consider the following problem

$$\begin{aligned} \max_{R_0,R_s} \quad & \eta(R_0,R_s) \\ \text{s.t.} \quad & P_s \leq \xi_s, \quad P_e \leq \xi_e. \end{aligned} \tag{27}$$

In addition to the service requirement of confidentiality, problem (27) also imposes a probabilistic service requirement on the connection outage, i.e., at least a fraction $1-\xi_s$ of HARQ sessions are successful. The connection outage constraint ensures that, at the expense of possibly lower average throughput, the delay constraint (that a packet can be delivered within M transmissions) is satisfied $1-\xi_s$ of the time, hence enabling applications which trade average rate for decoding delay like voice communication systems, e.g., CDMA2000 [24]. A similar constraint has been considered in [25] in terms of *service outage* for parallel fading channels.

To evaluate $p[m]$, P_e and P_s, we need the cumulative distribution functions (CDFs) of $I_{XY}(m)$ and $I_{XZ}(m)$. For the RTD protocol, we can use the fact that $\sum_{i=1}^{m}\lambda_i$ and $\sum_{i=1}^{m}\nu_i$ are gamma distributed to express the CDFs of $I_{XY}^{[\mathrm{RTD}]}(m)$ and $I_{XZ}^{[\mathrm{RTD}]}(m)$ in terms of incomplete gamma functions. In the case of the INR protocol, the distributions of $I_{XY}^{[\mathrm{INR}]}(m)$ and $I_{XZ}^{[\mathrm{INR}]}(m)$ cannot be written in a closed form. Hence, we resort to Monte-Carlo simulation in order to obtain empirical CDFs. Note that Monte Carlo simulation is needed only to estimate empirical CDFs, while (R_0^*, R_s^*) is found numerically by a (non-random) search.

VI. Asymptotic Analysis

In general, the secrecy throughput of the INR protocol is difficult to calculate since there is no closed form available for $\Pr\{I_{XY}(m) < R_0\}$. In this section, we consider the asymptotic secrecy throughput, which does have a closed form.

We are interested in asymptotic results as M increases without bound. Note that this asymptote corresponds to a delay-unconstrained system. In this case, secure HARQ protocols yield zero packet loss probability, i.e., the transmission of a codeword ends only when it is correctly decoded. As a result, the problems (26) and (27) yield the same throughput, which can be obtained from (24) as follows:

$$\eta(R_0, R_s) = \frac{MR_s}{\mathbb{E}[\mathcal{M}]} = \frac{MR_s}{1 + \sum_{m=1}^{M} \Pr\{I_{XY}(m) < R_0\}}. \tag{28}$$

Let us consider how to choose a mother Wyner code for the INR protocol in order to meet reliability and confidentiality constraints when M is large. Let λ and ν denote the instantaneous SNRs at the legitimate receiver and the eavesdropper, respectively.

Lemma 2. *Consider an INR secure HARQ protocol with the mother Wyner code $C \in \mathcal{C}(R_0, R_s, MN)$. Then*

$$\lim_{M\to\infty} P_e^{[\mathrm{INR}]} = 0 \quad \textit{and} \quad \lim_{M\to\infty} P_s^{[\mathrm{INR}]} = 0, \tag{29}$$

if and only if

$$\begin{aligned} R_0 &\le \frac{1}{2}\mathbb{E}[\log_2(1+\lambda)] \\ \textit{and} \qquad R_0 - R_s &\ge R_0 \frac{\mathbb{E}[\log_2(1+\nu)]}{\mathbb{E}[\log_2(1+\lambda)]}, \end{aligned} \tag{30}$$

where the expectations are over λ and/or ν. Furthermore, if (30) does not hold, then

$$\textit{either} \quad \lim_{M\to\infty} P_e^{[\mathrm{INR}]} = 1 \quad \textit{or} \quad \lim_{M\to\infty} P_s^{[\mathrm{INR}]} = 1. \tag{31}$$

Proof: A proof of Lemma 2 is given in Appendix C. ■

For comparison, we consider the situation in which the Wyner code C is transmitted over M-block fading channel without using the HARQ protocol. We refer to this case as the M-fading-block (MFB) coding scheme. Theorem 1 implies that, by using the MFB scheme, the requirement (29) can be achieved if and only if

$$\begin{aligned} R_0 &\le \frac{1}{2}\mathbb{E}[\log_2(1+\lambda)] \\ \text{and} \qquad R_0 - R_s &\ge \frac{1}{2}\mathbb{E}[\log_2(1+\nu)]. \end{aligned} \tag{32}$$

We note that the condition (30) for the INR protocol is weaker than the condition (32) for the MFB scheme. In other words, the INR scheme can achieve the confidentiality and reliability requirements more easily than can the MFB coding scheme by using the same Wyner code. This result illustrates the benefit of the INR secure HARQ protocol.

Based on Lemma 2, we have the following asymptotic result concerning the achievable throughput for secure HARQ protocols.

Theorem 3. *We consider the secure HARQ protocols over a block-fading wire-tap channel. If the secrecy information rate R_0 satisfies*

$$\lim_{M\to\infty} \frac{1}{MR_s} = 0, \tag{33}$$

then the secrecy throughput of RTD and INR protocols can be written as follows:

$$\lim_{M\to\infty} \max_{R_0,R_s} \eta(R_0, R_s) = \begin{cases} 0 & \textit{RTD} \\ (1/2)\mathbb{E}\left[\log_2(1+\lambda) - \log_2(1+\nu)\right] & \textit{INR} \end{cases},$$

where λ and ν are the instantaneous SNRs at the legitimate receiver and the eavesdropper, respectively.

Proof: We provide a proof in Appendix D. ■

We note that the RTD protocol involves suboptimal coding schemes, for which $\mathbb{E}[\mathcal{M}]$ grows faster than MR_s in (28). Hence, the limiting secrecy throughput η is zero. Theorem 3 again asserts the benefit of INR over RTD.

VII. Numerical Results

In our numerical examples, we consider Rayleigh block fading, i.e. the main channel instantaneous SNR λ has the probability density function (PDF) $f(\lambda) = (1/\bar{\lambda})e^{-\lambda/\bar{\lambda}}$, and the eavesdropper channel instantaneous SNR ν has the PDF $f(\nu) = (1/\bar{\nu})e^{-\nu/\bar{\nu}}$, where $\bar{\lambda}$ and $\bar{\nu}$ are the average SNRs of the main and eavesdropper channels, respectively.

To illustrate how the secrecy throughput η is related to the choice of R_0 (and R_s), we give a numerical example of η versus R_0 in Fig. 3, in which the parameter settings are as follows: the main channel average SNR $\bar{\lambda}$ is 15dB, the eavesdropper channel average SNR $\bar{\nu}$ is 5dB, the maximum number of transmissions M is 8. (We observe that similar results are obtained by using other parameter settings.) For each R_0, we obtain the maximum $R_s^*(R_0)$ that meets the secrecy constraint $\xi_s = 1, 10^{-2}$ or 10^{-4}, respectively. When there is no secrecy constraint ($\xi_s = 1$), due to the sub-optimality of the RTD scheme, the RTD curve is uniformly below the INR curve. This does not happen when there is a secrecy constraint. The reason

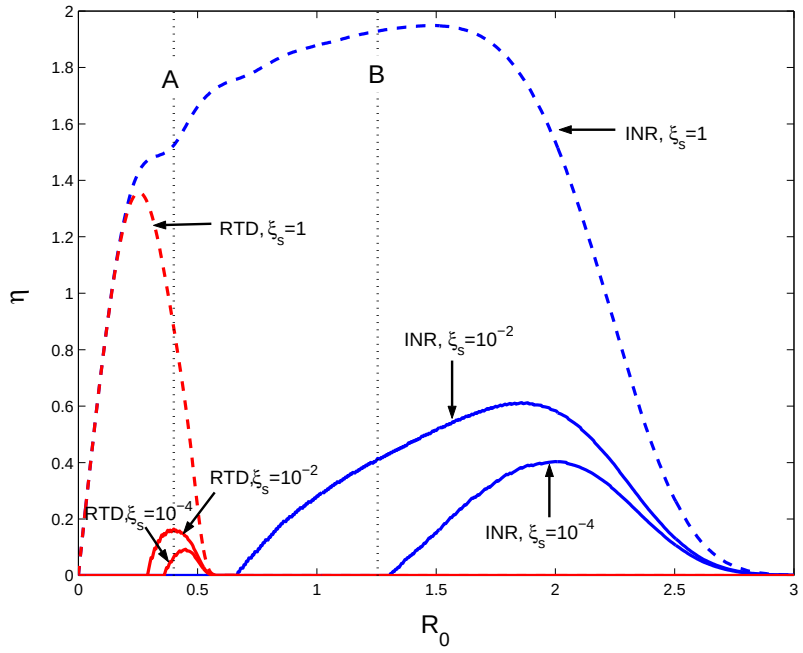

Fig. 3. Secrecy throughput η versus the main channel code rate R_0 under different secrecy requirements ξ_s, where the main channel average SNR is 15dB, the eavesdropper channel average SNR is 5dB, and the maximum number of transmissions is $M = 8$.

is that INR not only favors the information transmission to the intended receiver, but also benefits the eavesdropping by the eavesdropper. Hence, INR needs to sacrifice a larger portion of the main channel code rate than RTD in order to keep the eavesdropper ignorant of the confidential messages. This is reflected in Fig. 3 that a larger R_0 has to be chosen for INR (than RTD) in order to obtain a positive secrecy throughput.

It is clear from Fig. 3 that there exists a unique R_0^* (and therefore $R_s^*(R_0^*)$) to maximize η for each parameter setting. For all secrecy constraints ($\xi_s = 1, 10^{-2}$ or 10^{-4}), if the best R_0^* and $R_s^*(R_0^*)$ are chosen for each scheme accordingly, INR yields higher secrecy throughput than RTD does, which shows the benefit of INR over RTD.

According to (21), the choice of R_0 decides the reliability performance. This is shown in Fig. 4, where we plot the connection outage probability P_e versus the value of R_0. For both INR and RTD, P_e increases with the value of R_0. Note that a more strict secrecy constraint requires a larger R_0^* (as shown in Fig. 3), which however causes the degradation of the reliability performance. We can see that there exists a

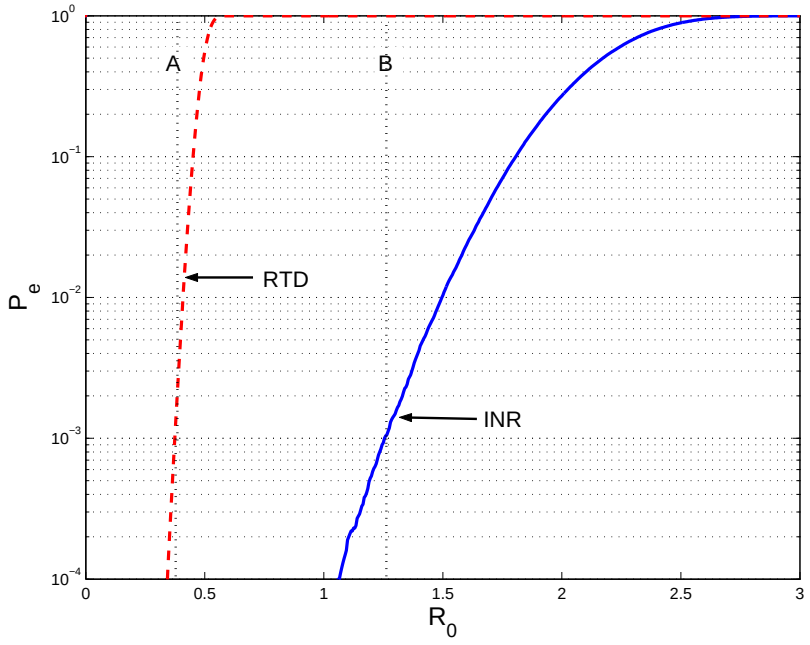

Fig. 4. Connection outage probability P_e versus the main channel code rate R_0, where the main channel average SNR is 15dB, the eavesdropper channel average SNR is 5dB, and $M = 8$.

tradeoff between secrecy and reliability.

Given a strict connection outage constraint $P_e < \xi_e$, the choice of R_0^* (and $R_s^*(R_0^*)$) might not be feasible. For instance, in order to obtain $P_e < 10^{-3}$, we need to choose $R_0^{[\mathrm{RTD}]} \leq 0.38$ and $R_0^{[\mathrm{INR}]} \leq 1.25$ (marked with 'A' and 'B' respectively in Fig. 3 and Fig. 4). Specifically, for a connection outage constraint $P_e < 10^{-3}$, R_0^* is not feasible for INR when $\xi_s = 10^{-2}$, and R_0^* is not feasible for both INR and RTD when $\xi_s = 10^{-4}$ in Fig. 3. Note that for the case of $\xi_s = 10^{-4}$ (and $\xi_e = 10^{-3}$), positive secrecy throughput cannot be obtained for INR, but can be obtained for RTD. This implies that RTD might outperform INR, when we have strict secrecy and connection outage constraints. This is a surprising result in the view of the well-known HARQ performance when there is no secrecy constraint, where INR always outperforms RTD [1].

In Fig. 5 and Fig. 6, we show the secrecy throughput η under different target secrecy outage probabilities ξ_s. There is no connection outage requirement in Fig. 5. There is an additional connection outage requirement of $p_e \leq \xi_e = 10^{-3}$ in Fig. 6. The parameter settings are $\bar{\lambda} = 15$dB, $\bar{\nu} = 5$dB and $M = 8$. We can see that small secrecy outage probability can be achieved when the throughput is small for both protocols. The INR protocol outperforms the RTD protocol uniformly when there is no connection

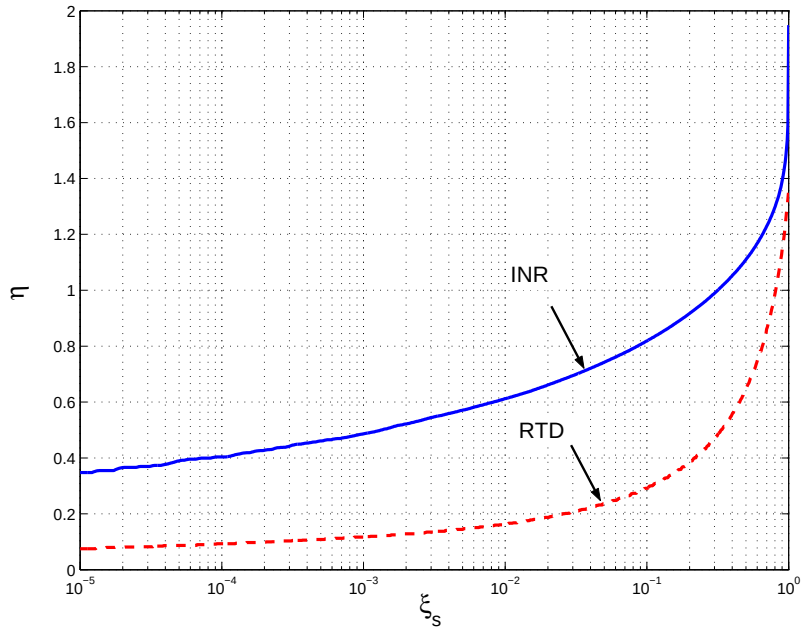

Fig. 5. Throughput η versus target secrecy outage probability ξ_s, when the main channel average SNR is 15dB, the eavesdropper channel average SNR is 5dB, and $M = 8$.

outage requirement. However, when there is a strict connection outage requirement, the RTD protocol outperforms the INR protocol when ξ_s is small (e.g., $\xi_s \leq 10^{-4}$).

Fig. 7 illustrates the relationship between the secrecy throughput η and the main channel average SNR $\bar{\lambda}$ when there is a target secrecy outage probability $\xi_s = 10^{-3}$ and no connection outage requirement. The average SNR of the eavesdropper channel is fixed to be 5dB. We find that the INR protocol outperforms the RTD protocol significantly, especially when the main channel SNR is large.

In Fig. 8, we show the secrecy throughput η versus the maximum number of transmissions M. Comparing with the secrecy throughput without the connection outage constraint, the secrecy throughput with a connection outage constraint ($P_e \leq 10^{-3}$) suffers some loss when M is small due to insufficient diversity. Both secrecy throughputs converge when sufficient diversity can be obtained as M increases. In particular, when $M \to \infty$, both throughputs are the same and are given by (28) in the asymptotic analysis. For INR, the secrecy throughput $\eta^{[\mathrm{INR}]}$ increases monotonically with M. For RTD, $\eta^{[\mathrm{RTD}]}$ decreases with M due to its strongly suboptimal coding scheme. This concurs with the asymptotic analysis that, when $M \to \infty$, a constant (nonzero) secrecy throughput ($0.5 * \mathbb{E}\left[\log_2(1+\lambda) - \log_2(1+\nu)\right] = 1.31$ according to Theorem 3) can be achieved for INR, while zero throughput can be obtained for RTD.

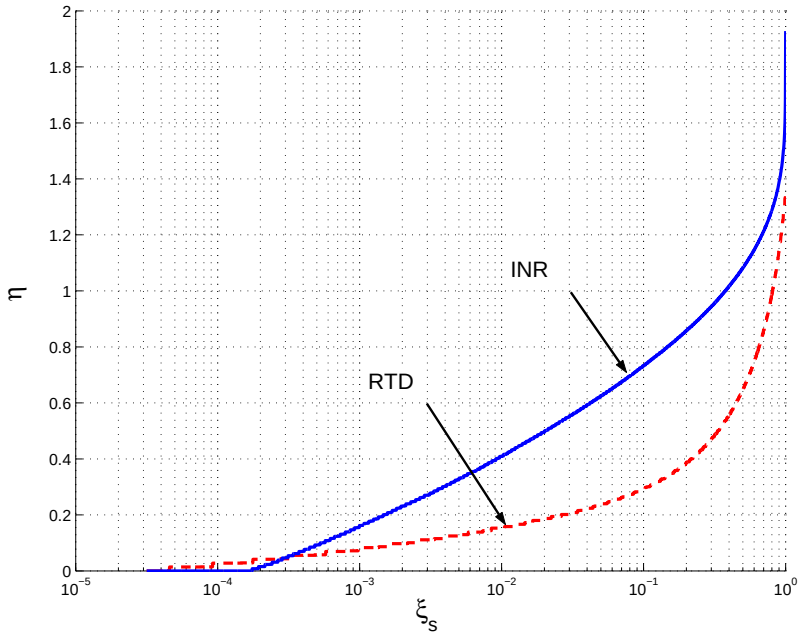

Fig. 6. Throughput η versus target secrecy outage probability ξ_s under connection outage probability $\xi_e = 10^{-3}$, when the main channel average SNR is 15dB, the eavesdropper channel average SNR is 5dB, and $M = 8$.

VIII. Conclusions and Future Directions

In this paper, we have studied secure packet communication over frequency-flat block-fading Gaussian channels, based on secure HARQ protocols with the joint consideration of channel coding, secrecy coding and retransmission protocols. From an information theoretic point of view, we have considered two secure HARQ protocols: a repetition time diversity scheme with maximal-ratio combining (RTD), and an incremental redundancy scheme based on rate-compatible Wyner secrecy codes (INR). We have proved the existence of good Wyner code sequences, which ensure that the legitimate receiver can decode the message and the eavesdropper can be kept ignorant of it for an HARQ session under certain channel realizations.

To facilitate the formulation of the outage-based throughput, we have defined two types of outage: connection outage and secrecy outage. The outage probabilities, more specifically, the connection and secrecy outage probabilities have been used to characterize the tradeoff between the reliability of the legitimate communication link and the confidentiality with respect to the eavesdropper's link. We have evaluated the achievable throughput of RTD and INR protocols under probabilistic requirements (constraints) on secrecy outage and/or connection outage, and have illustrated the benefits of HARQ schemes

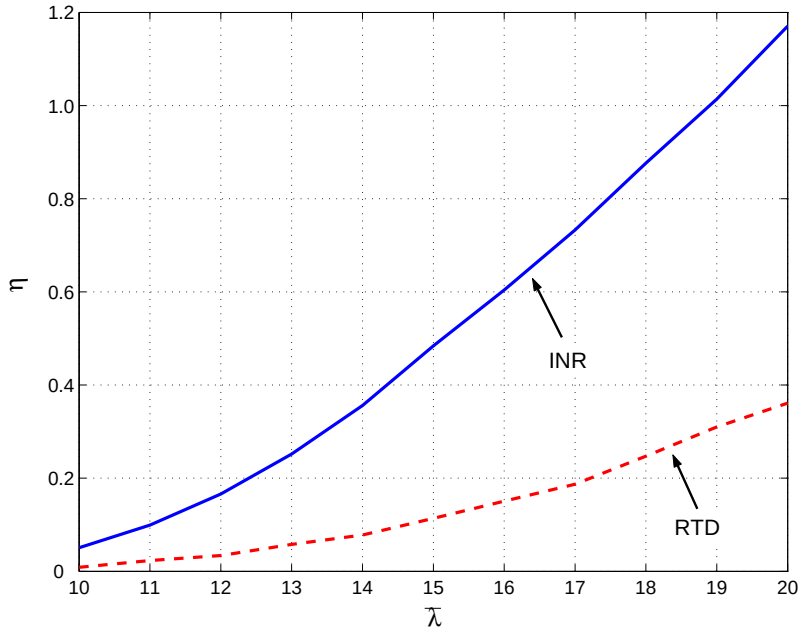

Fig. 7. Throughput η versus main channel average SNR $\bar{\lambda}$ under a target secrecy outage probability $\xi_s = 10^{-3}$, when the eavesdropper channel average SNR is 5dB and $M = 8$.

to information secrecy through some numerical results and an asymptotic analysis.

In general, INR can achieve a significantly larger throughput than RTD, which concurs with the results not involving secrecy that mutual-information accumulation (INR) is a more effective approach than SNR-accumulation (RTD). However, when one is forced to ensure small connection outage for the main channel even when it is bad, one is forced to reduce the main channel code rate. The INR scheme, having a larger coding gain (to both the intended receiver and the eavesdropper), needs to sacrifice a larger portion of the main channel code rate (i.e., requires a larger secrecy gap) in order to satisfy the secrecy requirement. Hence when the main channel code rate is bounded due to the connection outage constraint, the achievable secrecy throughput of INR may be smaller than that of RTD.

We conclude this work by pointing out some future research directions.

First, as pointed out in [26], many practical encoders are separated from the modulator and therefore the performance of HARQ protocols is impacted by modulation constraints. Although we have assumed Gaussian signaling, it is possible and also meaningful to extend the analysis to take discrete signaling into account.

In our analysis, we have assumed random coding and typical set decoding. Future work should consider

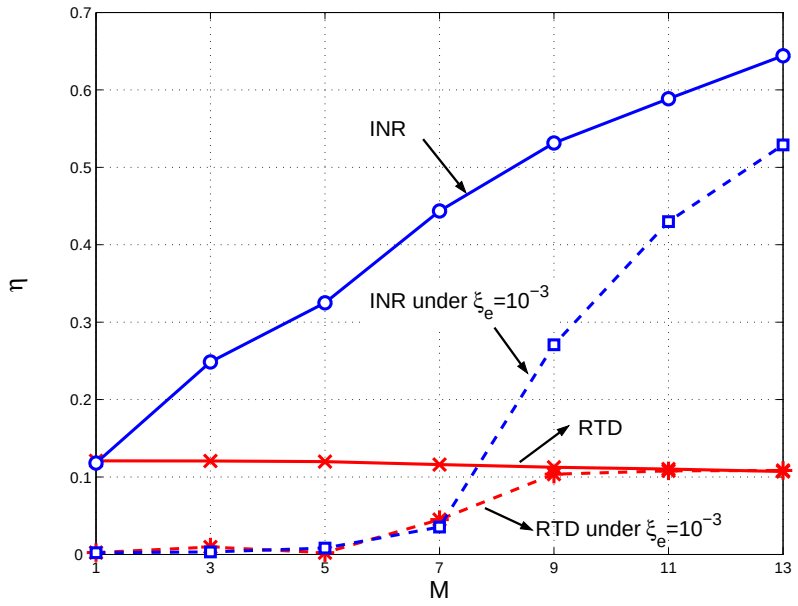

Fig. 8. Throughput η versus the maximum number of transmissions M under a target secrecy outage probability $\xi_s = 10^{-3}$, when the main and eavesdropper channel average SNRs are 15dB and 5dB, respectively.

practical coding and decoding schemes for secure HARQ protocols. Existing work on the practical secrecy code design includes coset coding [27], low-density parity check (LDPC) code design [28], and nested codes [29]. The design of practical rate compatible secrecy codes for Gaussian channels remains a challenging problem.

APPENDIX A
PROOF OF THEOREM 1

For convenience, let $\mathbf{p} \triangleq (\mathbf{h}, \mathbf{g})$ and $\mathcal{P}_*$ denote the set of channel pairs $(\mathbf{h}, \mathbf{g})$ so that

$$\frac{1}{M}\sum_{i=1}^{M} I(X;Y|h_i) = R_0 + \delta \tag{34}$$

and

$$\frac{1}{M}\sum_{i=1}^{M} I(X;Z|g_i) = R_0 - R_s + \delta, \tag{35}$$

where $\delta > 0$ is arbitrarily small. It is clear that $\mathcal{P}_* \subseteq \mathcal{P}$ when $\delta \to 0$.

In order to prove Theorem 1, we first consider the following lemma.

Lemma A.1. *There exists a code $C \in \mathcal{C}(R_0, R_s, MN)$ that is good for any channel pair $\mathbf{p} \in \mathcal{P}_*$.*

A. Proof of Lemma $A.1$

Proof: Following standard continuity arguments [22], we consider a quantization of the input and output of the channel (1) and work on the resulting discrete channel. Given a channel pair $\mathbf{p} = (\mathbf{h}, \mathbf{g})$, on every fading block $i \in [1, M]$, the channel is time-invariant and memoryless. Let $\mathbf{x}$ denote the input, and let $\mathbf{y}$ and $\mathbf{z}$ denote the outputs at the legitimate receiver and the eavesdropper, respectively. From the weak law of large numbers, we have the following limits in probability:

$$\lim_{N\to\infty} \frac{1}{N} \log_2 \Pr(\mathbf{x}) = -MH(X),$$

$$\lim_{N\to\infty} \frac{1}{N} \log_2 \Pr(\mathbf{y}) = -\sum_{i=1}^{M} H(Y|h_i),$$

$$\lim_{N\to\infty} \frac{1}{N} \log_2 \Pr(\mathbf{z}) = -\sum_{i=1}^{M} H(Z|g_i),$$

$$\lim_{N\to\infty} \frac{1}{N} \log_2 \Pr(\mathbf{x}, \mathbf{y}) = -\sum_{i=1}^{M} H(X, Y|h_i),$$

and

$$\lim_{N\to\infty} \frac{1}{N} \log_2 \Pr(\mathbf{x}, \mathbf{z}) = -\sum_{i=1}^{M} H(X, Z|g_i),$$

where $H(X)$ is the input entropy per letter; $H(Y|h_i)$ and $H(Z|g_i)$ are the output entropy per letter at the intended receiver and the eavesdropper, respectively, in block $i = 1, \ldots, M$; and $H(X, Y|h_i)$ and $H(X, Z|g_i)$ are the joint entropies per letter in block i. Define the typical set T_ϵ^N as the set of all sequences $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ for which the above sample means are within ϵ of their limits.

The random coding ensemble $\mathcal{C} = \mathcal{C}(R_0, R_s, MN)$ is constructed by generating 2^{NMR_0} codewords $\mathbf{x}(w, v)$, where $w = 1, 2, \ldots, 2^{NMR_s}$ and $v = 1, 2, \ldots, 2^{NM(R_0-R_s)}$, by choosing the $(MN)2^{NMR_0}$ symbols independently at random. Given $w \in \mathcal{W} = \{1, 2, \ldots, 2^{NMR_s}\}$, the encoder randomly and uniformly selects a v from $\{1, 2, \ldots, 2^{NM(R_0-R_s)}\}$ and transmits $\mathbf{x}(w, v)$.

1) Error Analysis: Given a message $w \in \mathcal{W}$, the legitimate receiver declares that $\mathbf{x}$ was transmitted, if $\mathbf{x}$ is the only codeword that is jointly typical with $\mathbf{y}$. An error is declared if either $\mathbf{x}$ is not jointly typical with $\mathbf{y}$, or there is another codeword $\tilde{\mathbf{x}}$ jointly typical with $\mathbf{y}$. Let us denote this type of error as $\mathcal{E}_1$. By following the same steps in [22, Theorem 8.7.1], we obtain that $\mathbb{E}_{C\in\mathcal{C}}[\Pr(\mathcal{E}_1|\mathbf{p}, C)]$, the probability of error $\mathcal{E}_1$ averaged over the code ensemble $\mathcal{C}$ is

$$\begin{aligned}
\mathbb{E}_{C\in\mathcal{C}}[\Pr(\mathcal{E}_1|\mathbf{p}, C)] &\leq \mathbb{E}\left\{ \Pr\left[(\mathbf{x}, \mathbf{y}) \notin T_\epsilon^N(P_{XY})\right] + \sum_{\tilde{\mathbf{x}}\neq\mathbf{x}} \Pr\left[(\tilde{\mathbf{x}}, \mathbf{y}) \in T_\epsilon^N(P_{XY})\right] \right\} \\
&\leq \epsilon + (2^{NMR_0} - 1)\mathbb{E}\left\{\Pr\left[(\tilde{\mathbf{x}}, \mathbf{y}) \in T_\epsilon^N(P_{XY})\right]\right\}
\end{aligned}$$

$$\begin{aligned} &= \epsilon + (2^{NMR_0} - 1)2^{-N\left[\sum_{i=1}^{M} I(X;Y|h_i) - \epsilon\right]} \\ &\leq \epsilon + 2^{-N(\delta-\epsilon)}. \end{aligned}$$

By choosing $\delta > \epsilon$, we have

$$\mathbb{E}_{C\in\mathcal{C}}[\Pr(\mathcal{E}_1|\mathbf{p}, C] \leq \epsilon_1, \tag{36}$$

for every channel pair $\mathbf{p} \in \mathcal{P}_*$ as the codeword length N is sufficiently large, where $\epsilon_1 = \epsilon + 2^{-N(\delta-\epsilon)}$.

Let $B(w)$ denote the set of codewords corresponding to message $w \in \mathcal{W}$ (bin w). Suppose that the eavesdropper gets to know w a priori, based on which it tries to determine which codeword was sent. The eavesdropper declares that $\mathbf{x}$ was sent, if $\mathbf{x}$ is the only codeword in $B(w)$ that is jointly typical with $\mathbf{z}$. An error is declared if either $\mathbf{x}$ is not jointly typical with $\mathbf{z}$, or there is another codeword $\tilde{\mathbf{x}}$ in $B(w)$ jointly typical with $\mathbf{z}$. Denoting this type of error as $\mathcal{E}_2$, we obtain that $\mathbb{E}_{C\in\mathcal{C}}[\Pr(\mathcal{E}_2|\mathbf{p}, C)]$, the average probability of error averaged over the code ensemble $\mathcal{C}$ is

$$\begin{aligned} \mathbb{E}_{C\in\mathcal{C}}[\Pr(\mathcal{E}_2|\mathbf{p}, C)] &\leq \mathbb{E}\left\{\Pr\left[(\mathbf{x},\mathbf{z}) \notin T_\epsilon^N(P_{XY})\right] + \sum_{\tilde{\mathbf{x}}\neq\mathbf{x}} \Pr\left[(\tilde{\mathbf{x}},\mathbf{z}) \in T_\epsilon^N(P_{XZ}), \tilde{\mathbf{x}} \in B(w)\right]\right\} \\ &\leq \epsilon + (2^{NMR_0} - 1)\mathbb{E}\left\{\Pr\left[(\tilde{\mathbf{x}},\mathbf{z}) \in T_\epsilon^N(P_{XZ})\right]\Pr\left[\tilde{\mathbf{x}} \in B(w)\right]\right\} \\ &\leq \epsilon + 2^{NM(R_0-R_s)}2^{-N\left[\sum_{i=1}^{M} I(X;Z|g_i) - \epsilon\right]} \\ &\leq \epsilon + 2^{-N(\delta-\epsilon)}. \end{aligned}$$

By choosing $\delta > \epsilon$, we have

$$\mathbb{E}_{C\in\mathcal{C}}[\Pr(\mathcal{E}_2|\mathbf{p}, C] \leq \epsilon_2 \tag{37}$$

for every channel pair $\mathbf{p} \in \mathcal{P}_*$ when the codeword length N is sufficiently large, where $\epsilon_2 = \epsilon + 2^{-N(\delta-\epsilon)}$.

Now we define an error event $\mathcal{E}$, which occurs whenever $\mathcal{E}_1$ or $\mathcal{E}_2$ occurs, i.e.

$$\mathcal{E} \triangleq \mathcal{E}_1 \cup \mathcal{E}_2. \tag{38}$$

According to (36) and (37), by using the union bound, we have for any $\mathbf{p} \in \mathcal{P}_*$,

$$\begin{aligned} \mathbb{E}_{C\in\mathcal{C}}[\Pr(\mathcal{E}|\mathbf{p}, C)] &\leq \mathbb{E}_{C\in\mathcal{C}}[\Pr(\mathcal{E}_1|\mathbf{p}, C)] + \mathbb{E}_{C\in\mathcal{C}}[\Pr(\mathcal{E}_2|\mathbf{p}, C)] \\ &\leq \epsilon_1 + \epsilon_2 = \epsilon_3. \end{aligned}$$

It is clear that the average error probability, averaged over the channel set $\mathcal{P}_*$ is

$$\mathbb{E}_{\mathbf{p}\in\mathcal{P}_*}\left[\mathbb{E}_{C\in\mathcal{C}}[\Pr(\mathcal{E}|\mathbf{p}, C)]\right] \leq \epsilon_3.$$

Interchanging expectations with respect to $\mathbf{p} \in \mathcal{P}_*$ and with respect to $C \in \mathcal{C}$ (since the integrand is nonnegative and bounded by 1) yields

$$\mathbb{E}_{C\in\mathcal{C}}\left[\mathbb{E}_{\mathbf{p}\in\mathcal{P}_*}[\Pr(\mathcal{E}|\mathbf{p},C)]\right] \leq \epsilon_3.$$

Then, there exists a sequence of codes $C^* \in \mathcal{C}$ (for increasing N) such that

$$\mathbb{E}_{\mathbf{p}\in\mathcal{P}_*}[\Pr(\mathcal{E}|\mathbf{p},C^*)] \leq \epsilon_3,$$

where $\Pr(\mathcal{E}|\mathbf{p},C^*)$ is a random variable that is a function of the channel pair $\mathbf{p}$. According to the Markov inequality, we have

$$\Pr\left(\Pr(\mathcal{E}|\mathbf{p},C^*) \geq \sqrt{\epsilon_3}\right) \leq \frac{\mathbb{E}_{\mathbf{p}\in\mathcal{P}_*}[\Pr(\mathcal{E}|\mathbf{p},C^*)]}{\sqrt{\epsilon_3}} \leq \frac{\epsilon_3}{\sqrt{\epsilon_3}} = \sqrt{\epsilon_3}.$$

By letting $\sqrt{\epsilon_3} = \epsilon_4$ (ϵ_4 is still arbitrarily small), we obtain that, for any $\mathbf{p} \in \mathcal{P}_*$,

$$\Pr\left(\Pr(\mathcal{E}|\mathbf{p},C^*) \geq \epsilon_4\right) \leq \epsilon_4$$

$$\text{or} \qquad \Pr\left(\Pr(\mathcal{E}|\mathbf{p},C^*) < \epsilon_4\right) \geq 1-\epsilon_4. \tag{39}$$

Since $\Pr(\mathcal{E}_1|\mathbf{p},C^*)$ and $\Pr(\mathcal{E}_2|\mathbf{p},C^*)$ are both upper bounded by $\Pr(\mathcal{E}|\mathbf{p},C^*)$, we have that

$$\Pr\left(\Pr(\mathcal{E}_1|\mathbf{p},C^*) < \epsilon_4\right) \geq 1-\epsilon_4 \tag{40}$$

$$\text{and} \qquad \Pr\left(\Pr(\mathcal{E}_2|\mathbf{p},C^*) < \epsilon_4\right) \geq 1-\epsilon_4. \tag{41}$$

According to (40), there exists a (non-random) sequence of codes $C^* \in \mathcal{C}(R_0, R_s, MN)$, which when used, the legitimate receiver can decode the message with arbitrarily small error probability for all $\mathbf{p} \in \mathcal{P}_*$ with probability 1. Inequality (41) will be used in the equivocation calculation as followed.

2) Equivocation Calculation: Now we calculate the equivocation rate to check whether the perfect secrecy requirement can be satisfied when codebook C^* is used.

We bound the equivocation at the eavesdropper as follows:

$$\begin{aligned}
H(W|\mathbf{Z},\mathbf{h},\mathbf{g}) &= H(W,\mathbf{Z}|\mathbf{h},\mathbf{g}) - H(\mathbf{Z}|\mathbf{h},\mathbf{g}) \\
&= H(W,\mathbf{Z},\mathbf{X}|\mathbf{h},\mathbf{g}) - H(\mathbf{Z}|\mathbf{h},\mathbf{g}) - H(\mathbf{X}|W,\mathbf{Z},\mathbf{h},\mathbf{g}) \\
&= H(\mathbf{X}|\mathbf{h},\mathbf{g}) + H(W,\mathbf{Z}|\mathbf{X},\mathbf{h},\mathbf{g}) - H(\mathbf{Z}|\mathbf{h},\mathbf{g}) - H(\mathbf{X}|W,\mathbf{Z},\mathbf{h},\mathbf{g}) \\
&\geq H(\mathbf{X}|\mathbf{h},\mathbf{g}) - I(\mathbf{X};\mathbf{Z}|\mathbf{h},\mathbf{g}) - H(\mathbf{X}|W,\mathbf{Z},\mathbf{h},\mathbf{g}).
\end{aligned}$$

For the first term, we notice that

$$H(\mathbf{X}|\mathbf{h},\mathbf{g}) = NMR_0. \tag{42}$$

To bound the second term, we define

$$\mu(\mathbf{X},\mathbf{Z}|\mathbf{h},\mathbf{g}) = \begin{cases} 1 & \text{if } (\mathbf{X},\mathbf{Z}) \notin T_\epsilon^N(P_{XZ}) \\ 0 & \text{otherwise.} \end{cases}$$

Now

$$\begin{aligned} I(\mathbf{X};\mathbf{Z}|\mathbf{h},\mathbf{g}) &\leq I(\mathbf{X},\mu;\mathbf{Z}|\mathbf{h},\mathbf{g}) \\ &= I(\mathbf{X};\mathbf{Z}|\mathbf{h},\mathbf{g},\mu) + I(\mu;\mathbf{Z}|\mathbf{h},\mathbf{g}) \\ &= \sum_{j=0}^{1} \Pr(\mu=j) I(\mathbf{X};\mathbf{Z}|\mathbf{h},\mathbf{g},\mu=j) + I(\mu;\mathbf{Z}|\mathbf{h},\mathbf{g}). \end{aligned} \tag{43}$$

Note that $I(\mu;\mathbf{Z}|\mathbf{h},\mathbf{g}) \leq h(\mu) \leq 1$,

$$\begin{aligned} \Pr(\mu=1) I(\mathbf{X};\mathbf{Z}|\mathbf{h},\mathbf{g},\mu=1) &\leq N \Pr\left[(\mathbf{X},\mathbf{Z}) \notin T_\epsilon^N(P_{XZ})|\mathbf{h},\mathbf{g}\right] \log_2|Z| \\ &\leq N\epsilon \log_2|Z|, \end{aligned}$$

and

$$\begin{aligned} \Pr(\mu=0) I(\mathbf{X};\mathbf{Z}|\mathbf{h},\mathbf{g},\mu=0) &\leq I(\mathbf{X};\mathbf{Z}|\mathbf{h},\mathbf{g},\mu=0) \\ &= H(\mathbf{X}|\mathbf{h},\mathbf{g},\mu=0) + H(\mathbf{Z}|\mathbf{h},\mathbf{g},\mu=0) - H(\mathbf{X},\mathbf{Z}|\mathbf{h},\mathbf{g},\mu=0) \\ &\leq N\left[MH(X) + \sum_{i=1}^{M} H(Z|g_i) - \sum_{i=1}^{M} H(X,Z|g_i) + 3\epsilon\right] \\ &= N\left[\sum_{i=1}^{M} I(X;Z|g_i) + 3\epsilon\right]. \end{aligned}$$

Therefore, we can bound the second term as

$$\begin{aligned} I(\mathbf{X};\mathbf{Z}|\mathbf{h},\mathbf{g}) &\leq N\left[\sum_{i=1}^{M} I(X;Z|g_i) + (\log_2|Z|+3)\epsilon\right] + 1 \\ &= NM[R_0 - R_s + \delta - (\log_2|Z|+3)\epsilon - 1/N] \\ &= NM(R_0 - R_s + \delta_1). \end{aligned} \tag{44}$$

To bound the third term, we need to use (41), according to which the eavesdropper can decode $\mathbf{X}$ with arbitrarily small error probability, given that W is known in prior and $\mathbf{Z}$ is observed. Fano's inequality implies that

$$H(\mathbf{X}|W,\mathbf{Z},\mathbf{h},\mathbf{g}) \leq 1 + NM(R_0 - R_s)\Pr(\mathcal{E}_2|\mathbf{p},C^\star) \triangleq NM\delta_2 \tag{45}$$

for every channel pair $\mathbf{p} \in \mathcal{P}_*$.

Now we can combine (42), (44) and (45) into the equivocation calculation:

$$\begin{aligned} H(W|\mathbf{Z},\mathbf{h},\mathbf{g}) &\geq NMR_0 - NM(R_0 - R_s + \delta_1) - NM\delta_2 \\ &= NM(R_s - \delta_3). \end{aligned} \tag{46}$$

Note that the above equivocation calculation is obtained when (non-random) code C^* is used, instead of the random code ensemble $\mathcal{C}(R_0, R_s, MN)$. Equation (46) implies that the perfect secrecy requirement is met. This, together with the error probability analysis, implies that code C^* is good for all channel pairs $\mathbf{p} \in \mathcal{P}_*$ with probability 1. ■

B. Proof of Theorem 1

Proof: Now we show that code C^* is also good for any channel pair $\mathbf{p} \in \mathcal{P}$. Note that for every $\mathbf{p} = (\mathbf{h}, \mathbf{g}) \in \mathcal{P}$, there always exists *at least* a channel pair $\mathbf{p}_* = (\mathbf{h}_*, \mathbf{g}_*) \in \mathcal{P}_*$, such that $\mathbf{h} \succeq \mathbf{h}_*$ and $\mathbf{g} \preceq \mathbf{g}_*$. With the input $\mathbf{X}$, we denote the outputs from the channel $(\mathbf{h}, \mathbf{g})$ at the legitimate receiver and the eavesdropper by $\mathbf{Y}$ and $\mathbf{Z}$, respectively. We also denote by $\mathbf{Y}_1$ and $\mathbf{Z}_1$ the outputs at the corresponding receivers from $(\mathbf{h}_*, \mathbf{g}_*)$. Since code C^* is good for $(\mathbf{h}_*, \mathbf{g}_*)$, $\mathbf{Y}_1$ can be decoded with arbitrarily small error probability at the legitimate receiver and the equivocation at the eavesdropper with $\mathbf{Z}_1$ being observed satisfies

$$H(W|\mathbf{Z}_1, \mathbf{g}_*) \geq H(W) - N\epsilon \tag{47}$$

for all $\epsilon > 0$ and sufficiently large N. Since $\mathbf{h} \succeq \mathbf{h}_*$, $\mathbf{Y}_1$ is a degraded version of $\mathbf{Y}$, and thus if $\mathbf{Y}_1$ can be decoded at the legitimate receiver with arbitrarily small error probability, then so can $\mathbf{Y}$. We also have that

$$\begin{aligned} &H(W|\mathbf{Z},\mathbf{g}) - H(W|\mathbf{Z}_1,\mathbf{g}_*) \\ &= I(W;\mathbf{Z}_1|\mathbf{g}_*) - I(W;\mathbf{Z}|\mathbf{g}) \geq 0, \end{aligned}$$

where we use the fact that $\mathbf{Z}$ is a degraded version of $\mathbf{Z}_1$, since $\mathbf{g} \preceq \mathbf{g}_*$. Therefore,

$$H(W|\mathbf{Z},\mathbf{g}) \geq H(W|\mathbf{Z}_1,\mathbf{g}_*) \geq H(W) - N\epsilon, \tag{48}$$

for all $\epsilon > 0$ and sufficiently large N, which is the perfect secrecy requirement. ■

APPENDIX B
PROOF OF THEOREM 2

Proof: We note that the punctured code C_m is obtained by taking the first m blocks, $\mathbf{x}(m) = [x_1^N, \ldots, x_m^N]$, of the mother code C, where the block x_i^N is transmitted over a wire-tap channel with

channel pairs (h_i, g_i), for $i = 1, \ldots, m$. Based on the equivalent M-parallel channel model, we can form a new sequence of channel pairs by adding other $M - m$ dummy memoryless channels whose outputs are independent of the input. For example, we can let $h_i = 0$ and $g_i = 0$ for all $i = m+1, \ldots, M$. The dummy channel pairs have zero mutual information between the input and output; that is,

$$\sum_{i=1}^{M} I(X;Y|h_i) = \sum_{i=1}^{m} I(X;Y|h_i)$$

$$\text{and} \qquad \sum_{i=1}^{M} I(X;Z|g_i) = \sum_{i=1}^{m} I(X;Z|g_i).$$

Now, by using Theorem 1 and the fact $\mathcal{P}(m) \subseteq \mathcal{P}$, we have the desired result. ■

APPENDIX C
PROOF OF LEMMA 2

Applying the weak law of large numbers, we have the following lemma that is used in the proofs of Lemma 2 and Theorem 3.

Lemma C.1. *Let A_i be i.i.d. random variables with means μ_A and variances σ_A^2. Then, for alll $\epsilon > 0$,*

$$\lim_{M\to\infty} \Pr\left[\frac{1}{M}\sum_{i=1}^{M}(A_i - \mu_A) < \epsilon\right] = 1$$

$$\textit{and} \qquad \lim_{M\to\infty} \Pr\left[\frac{1}{M}\sum_{i=1}^{M}(A_i - \mu_A) < -\epsilon\right] = 0. \tag{49}$$

Now, we consider the proof of Lemma 2.

Proof: Define $A_i = (1/2)\log_2(1+\lambda_i)$ and its mean $\mu_A = \mathbb{E}[A_i]$, and $B_i = (1/2)\log_2(1+\nu_i)$ and its mean $\mu_B = \mathbb{E}[B_i]$, for $i = 1, \ldots, M$. The connection outage probability $P_e^{[\mathrm{INR}]}$, defined in (21), can be rewritten as follows:

$$\begin{aligned} P_e^{[\mathrm{INR}]} &= \Pr\left(\frac{1}{M}\sum_{i=1}^{M} A_i < R_0\right) \\ &= \Pr\left(\frac{1}{M}\sum_{i=1}^{M}(A_i - \mu_A) < R_0 - \mu_A\right). \end{aligned}$$

By using Lemma C.1, we have, for all $\epsilon > 0$,

$$\lim_{M\to\infty} P_e^{[\mathrm{INR}]} = \begin{cases} 0, & R_0 \le \mu_A - \epsilon \\ 1, & R_0 \ge \mu_A + \epsilon. \end{cases} \tag{50}$$

We first prove the sufficiency given by (29) in Lemma 2 and show that if

$$R_0 \leq \mu_A - \epsilon \quad \text{and} \quad R_0 - R_s \geq R_0 \left(\frac{\mu_B}{\mu_A - \epsilon} + \epsilon \right), \tag{51}$$

then (29) holds.

Define

$$M_1 = \left\lfloor \frac{MR_0}{\mu_A - \epsilon} \right\rfloor. \tag{52}$$

Note that (51) implies that $M_1 \leq M$. Hence, we can bound the secrecy outage probability $P_s^{[\mathrm{INR}]}$, defined in (22), as follows:

$$\begin{aligned}
P_s^{[\mathrm{INR}]} &= \sum_{m=1}^{M_1} p[m] \Pr\left(\frac{1}{M} \sum_{i=1}^{m} B_i \geq R_0 - R_s \right) + \sum_{m=M_1+1}^{M} p[m] \Pr\left(\frac{1}{M} \sum_{i=1}^{m} B_i \geq R_0 - R_s \right) \\
&\leq \left(\sum_{m=1}^{M_1} p[m] \right) \Pr\left(\frac{1}{M} \sum_{i=1}^{M_1} B_i \geq R_0 - R_s \right) + \sum_{m=M_1+1}^{M} p[m] \\
&\leq \Pr\left[\sum_{i=1}^{M_1} B_i \geq M(R_0 - R_s) \right] + \Pr\left(\sum_{i=1}^{M_1} A_i < MR_0 \right) \\
&= \Pr\left[\sum_{i=1}^{M_1} \frac{B_i - \mu_B}{M_1} \geq \frac{M(R_0 - R_s)}{M_1} - \mu_B \right] + \Pr\left(\sum_{i=1}^{M_1} \frac{A_i - \mu_A}{M_1} < \frac{MR_0}{M_1} - \mu_A \right) \\
&\leq \Pr\left[\sum_{i=1}^{M_1} \frac{B_i - \mu_B}{M_1} \geq \epsilon(\mu_A - \epsilon) \right] + \Pr\left(\sum_{i=1}^{M_1} \frac{A_i - \mu_A}{M_1} < \frac{MR_0}{M_1} - \mu_A \right)
\end{aligned} \tag{53}$$

where the last step follows from the condition (51) and the definition of M_1 in (52). Applying Lemma C.1, we have

$$\lim_{M \to \infty} \Pr\left[\sum_{i=1}^{M_1} \frac{B_i - \mu_B}{M_1} \geq \epsilon(\mu_A - \epsilon) \right] = 0 \tag{54}$$

and

$$\begin{aligned}
\lim_{M \to \infty} \left(\sum_{i=1}^{M_1} \frac{A_i - \mu_A}{M_1} < \frac{MR_0}{M_1} - \mu_A \right) &= \lim_{M \to \infty} \Pr\left(\sum_{i=1}^{M_1} \frac{A_i - \mu_A}{M_1} < -\epsilon \right) \\
&= 0.
\end{aligned} \tag{55}$$

Combining (50), (53), (54), and (55), we have (29).

Next, we prove the necessity given by (31) in Lemma 2. Based on (50) we need only to show that if

$$R_0 - R_s \leq R_0 \left(\frac{\mu_B}{\mu_A} - \epsilon \right) \quad \text{and} \quad R_0 < \mu_A + \epsilon, \tag{56}$$

then $\lim_{M\to\infty} P_s^{[\mathrm{INR}]} = 1$. Define

$$M_2 = \left\lceil \frac{M(R_0 - R_s)}{\mu_B - \epsilon_2} \right\rceil \tag{57}$$

where $\epsilon_2 = (\mu_A - \epsilon)\epsilon$. Note that the condition (56) implies that $M_2 \leq M$. In this case, we obtain the following lower bound on $P_s^{[\mathrm{INR}]}$:

$$\begin{aligned}
P_s^{[\mathrm{INR}]} &\geq \sum_{m=M_2}^{M} p[m] \Pr\left[\sum_{i=1}^{m} B_i \geq M(R_0 - R_s)\right] \\
&\geq \left(\sum_{m=M_2}^{M} p[m]\right) \Pr\left[\sum_{i=1}^{M_2} B_i \geq M(R_0 - R_s)\right] \\
&= \Pr\left(\sum_{i=1}^{M_2-1} A_i < MR_0\right) \Pr\left[\sum_{i=1}^{M_2} B_i \geq M(R_0 - R_s)\right] \\
&= \Pr\left(\sum_{i=1}^{M_2-1} \frac{A_i - \mu_A}{M_2 - 1} < \frac{MR_0}{M_2 - 1} - \mu_A\right) \Pr\left[\sum_{i=1}^{M_2} \frac{B_i - \mu_B}{M_2} \geq \frac{M(R_0 - R_s)}{M_2} - \mu_B\right].
\end{aligned} \tag{58}$$

Based on the condition (56) and the definitions of M_2 and ϵ_2, we have

$$\begin{aligned}
\frac{MR_0}{M_2 - 1} - \mu_A &= \frac{MR_0}{\lceil M(R_0 - R_s)/(\mu_B - \epsilon_2)\rceil - 1} - \mu_A \\
&\geq \frac{R_0}{R_0 - R_s}(\mu_B - \epsilon_2) - \mu_A \\
&\geq \frac{\mu_A \epsilon^2}{\mu_B - \epsilon\mu_A} \\
&> 0.
\end{aligned}$$

By applying Lemma C.1, we have

$$\lim_{M\to\infty} \Pr\left(\sum_{i=1}^{M_2-1} \frac{A_i - \mu_A}{M_2 - 1} < \frac{MR_0}{M_2 - 1} - \mu_A\right) = 1. \tag{59}$$

On the other hand, since

$$\frac{M(R_0 - R_s)}{M_2} - \mu_B \leq -\epsilon_2 < 0,$$

Lemma C.1 implies that

$$\lim_{M\to\infty} \Pr\left(\frac{1}{M_2}\sum_{i=1}^{M_2}(B_i - \mu_B) \geq \frac{R_0 - R_s}{M_2} - \mu_B\right) = 1. \tag{60}$$

Finally, combining (50), (58), (59), and (60), we have the necessity of Lemma 2. ■

APPENDIX D
PROOF OF THEOREM 3

To derive Theorem 3, we need the following lemmas from [1].

Lemma D.1. *Suppose A be a random variable with CDF F_A. Then, for all a and $\tilde{a}$. we have*

$$F_A(a) \leq F_A(\tilde{a}) + \mathbf{1}(a \geq \tilde{a}) \tag{61}$$

where $\mathbf{1}(\cdot)$ denote the indicator function.

Lemma D.2. *Suppose $\{A_i\}$ is a sequence of i.i.d. zero mean random variables with variances σ_A^2. Then, for all $\epsilon > 0$ and sufficiently large n,*

$$\Pr\left(\frac{1}{\sqrt{n}}\sum_{i=1}^{n} A_i < -\sqrt{n}\epsilon\right) \leq \exp\left(-n\frac{\epsilon^2}{2\sigma_A^2}\right). \tag{62}$$

We note that Lemma D.2 follows from the central limit theorem and the bound on the Gaussian tail function, $Q(a) \leq \exp(-a^2/2)$, where Q denotes the tail function of the standard Gaussian distribution.

A. INR Protocol

Proof: Again, we define $A_i = (1/2)\log_2(1+\lambda_i)$ with mean $\mu_A = \mathbb{E}[A_i]$ and variance σ_A^2, $B_i = (1/2)\log_2(1+\nu_i)$ with mean $\mu_B = \mathbb{E}[B_i]$, for $i = 1, \ldots, M$, and

$$M_4 = \left\lfloor \frac{MR_0}{\mu_A + \epsilon} \right\rfloor.$$

The reliability condition in (50) implies $M_4 \leq M$.

We first consider an upper bound of $\eta^{[\mathrm{INR}]}$ based on (28):

$$\begin{aligned}
\eta^{[\mathrm{INR}]} &\leq MR_s \left[\sum_{m=1}^{M_4} \Pr\left(\sum_{i=1}^{m} A_i < MR_0\right)\right]^{-1} \\
&\leq MR_s \left[\sum_{m=1}^{M_4} \Pr\left(\sum_{i=1}^{M_4} A_i < MR_0\right)\right]^{-1} \\
&= \frac{MR_s}{M_4}\left\{\Pr\left[\sum_{i=1}^{M_4}\frac{A_i - \mu_A}{M_4} < \frac{MR_0}{M_4} - \mu_A\right]\right\}^{-1}.
\end{aligned}$$

Since $MR_0/M_4 - \mu_A \geq \epsilon > 0$, according to Lemma C.1, we have

$$\lim_{M\to\infty} \Pr\left[\sum_{i=1}^{M_4}\frac{A_i - \mu_A}{M_4} < \frac{MR_0}{M_4} - \mu_A\right] = 1. \tag{63}$$

Hence,

$$\lim_{M\to\infty} \eta^{[\mathrm{INR}]} \leq \lim_{M\to\infty} \frac{MR_s}{M_4} = \frac{R_s}{R_0}\mu_A. \tag{64}$$

Next, we consider a lower bound on $\eta^{[\mathrm{INR}]}$. Let $M_5 = \lfloor MR_0/(\mu_A - \epsilon)\rfloor$. We have

$$\begin{aligned} \frac{1}{\eta^{[\mathrm{INR}]}} &\leq \frac{1}{MR_s} + \frac{1}{MR_s}\sum_{m=1}^{M}\left[\Pr\left(\sum_{i=1}^{m}\frac{A_i}{m} < \mu_A - \epsilon\right) + \mathbf{1}\left(\frac{MR_0}{m} \geq \mu_A - \epsilon\right)\right] \qquad (65)\\ &= \frac{1+L(M)}{MR_s} + \frac{M_5}{MR_s}, \end{aligned}$$

where (65) follows from Lemma D.1 and

$$L(M) = \sum_{m=1}^{M}\Pr\left(\frac{1}{m}\sum_{i=1}^{m}(A_i - \mu_A) < -\epsilon\right). \tag{66}$$

By Lemma D.2, there exists an integer n, finite and independent of R_0, so that

$$\begin{aligned} L(M) &= \sum_{m=1}^{n}\Pr\left(\frac{1}{m}\sum_{i=1}^{m}(A_i - \mu_A) < -\epsilon\right) + \sum_{m=n+1}^{M}\Pr\left(\frac{1}{m}\sum_{i=1}^{m}(A_i - \mu_A) < -\epsilon\right)\\ &\leq \sum_{m=1}^{n}\Pr\left(\frac{1}{m}\sum_{i=1}^{m}(A_i - \mu_A) < -\epsilon\right) + \sum_{m=n+1}^{\infty}\exp\left(-m\frac{\epsilon^2}{2\sigma_A^2}\right). \end{aligned}$$

Since the first sum contains a finite number of terms (each being less than 1), and the second converges for all $\epsilon > 0$, we have that

$$\lim_{M\to\infty}\frac{1+L(M)}{MR_s} = 0.$$

Hence, we have that

$$\lim_{M\to\infty} \eta^{[\mathrm{INR}]} \geq \lim_{M\to\infty} \frac{MR_s}{M_5} = \frac{R_s}{R_0}\mu_A. \tag{67}$$

Combining (64) and (67), we obtain

$$\lim_{M\to\infty} \eta^{[\mathrm{INR}]} = \frac{R_s}{R_0}\mu_A = \frac{R_s}{2R_0}\mathbb{E}\left[\log_2(1+\lambda)\right]. \tag{68}$$

Furthermore, Lemma 2 implies that

$$\frac{R_s}{R_0} \leq 1 - \frac{\mathbb{E}[\log_2(1+\nu)]}{\mathbb{E}[\log_2(1+\lambda)]}. \tag{69}$$

Finally, combining (68) and (69), we have the desired result that

$$\lim_{M\to\infty} \eta^{[\mathrm{INR}]} = \frac{1}{2}\mathbb{E}\left[\log_2(1+\lambda) - \log_2(1+\nu)\right].$$

■

B. RTD Scheme

Proof: We first consider the connection outage probability $P_e^{[\mathrm{RTD}]}$. Let $A_i = \lambda_i$ with mean $\mu_A = \mathbb{E}[\lambda_i]$, for $i = 1, \ldots, M$. Based on (21) we have

$$\begin{aligned} P_e^{[\mathrm{RTD}]} &= \Pr\left[\frac{1}{2M}\log_2\left(1+\sum_{i=1}^{M} A_i\right) < R_0\right] \\ &= \Pr\left(\sum_{i=1}^{M}\frac{A_i-\mu_A}{M} < \frac{2^{2MR_0}-1}{M} - \mu_A\right). \end{aligned}$$

By using Lemma C.1, we have, for all $\epsilon > 0$,

$$\lim_{M\to\infty} P_e^{[\mathrm{RTD}]} = \begin{cases} 0, & \frac{1}{M}(2^{2MR_0}-1) \le \mu_A - \epsilon \\ 1, & \frac{1}{M}(2^{2MR_0}-1) \ge \mu_A + \epsilon. \end{cases} \tag{70}$$

Hence, to ensure the connection outage requirement, R_0 should satisfy

$$\frac{2^{2MR_0}-1}{M} < \mu_A + \epsilon. \tag{71}$$

Now, we consider an upper bound on $\eta^{[\mathrm{RTD}]}$. Let

$$M_3 = \left\lfloor \frac{2^{2MR_0}-1}{\mu_A+\epsilon} \right\rfloor < M,$$

where the inequality follows from (71). By using (28), we have

$$\begin{aligned} \eta^{[\mathrm{RTD}]} &\le MR_s\left[1+\sum_{m=1}^{M_3}\Pr\left(\sum_{i=1}^{m} A_i < 2^{2MR_0}-1\right)\right]^{-1} \\ &\le MR_s\left[\sum_{m=1}^{M_3}\Pr\left(\sum_{i=1}^{M_3} A_i < 2^{2MR_0}-1\right)\right]^{-1} \\ &\le \frac{MR_0}{M_3}\left[\Pr\left(\sum_{i=1}^{M_3}\frac{A_i-\mu_A}{M_3} < \frac{2^{2MR_0}-1}{M_3} - \mu_A\right)\right]^{-1}. \end{aligned}$$

Since $(2^{2MR_0}-1)/M_3 - \mu_A \ge \epsilon > 0$ and Lemma C.1, we have that

$$\lim_{M\to\infty}\Pr\left(\sum_{i=1}^{M_3}\frac{A_i-\mu_A}{M_3} < \frac{2^{2MR_0}-1}{M_3} - \mu_A\right) = 1.$$

Therefore,

$$\lim_{M\to\infty}\eta^{[\mathrm{RTD}]} \le \lim_{M\to\infty}\frac{MR_0}{M_3} = \lim_{M\to\infty}\frac{MR_0(\mu_A+\epsilon_3)}{2^{2MR_0}-1} = 0.$$

■

REFERENCES

[1] G. Caire and D. Tuninetti, "The throughput of hybrid-ARQ protocols for the Gaussian collision channel," *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 1971–1988, Jul. 2001.

[2] J. Hagenauer, "Rate-compatible punctured convolutional codes (RCPC codes) and their applications," *IEEE Trans. Commun.*, vol. 36, no. 4, pp. 389–400, Apr. 1988.

[3] K. R. Narayanan and G. L. Stuber, "A novel ARQ technique using the turbo coding principle," *IEEE Commun. Lett.*, vol. 1, no. 2, pp. 49–51, Mar. 1997.

[4] D. Tuninetti and G. Caire, "The throughput of some wireless multiaccess systems," *IEEE Trans. Inf. Theory*, vol. 48, no. 5, pp. 2773–2785, Oct. 2002.

[5] E. Soljanin, R. Liu, and P. Spasojević, "Hybrid ARQ with random transmission assignments," in *Advances in Network Information Theory*, ser. DIMACS Series in Discrete Mathematics and Theoretical Computer Science, P. Gupta, G. Kramer, and A. J. van Wijngaarden, Eds. Providence, RI: American Mathematical Society, 2004, pp. 321–334.

[6] S. Sesia, G. Caire, and G. Vivier, "Incremental redundancy hybrid ARQ schemes based on low-density parity-check codes," *IEEE Trans. Commun.*, vol. 52, no. 8, pp. 1311–1321, Aug. 2004.

[7] C. F. Leanderson and G. Caire, "The performance of incremental redundancy schemes based on convolutional codes in the block-fading Gaussian collision channel," *IEEE Trans. Wireless Commun.*, vol. 3, no. 3, pp. 843–854, May 2004.

[8] E. Soljanin, N. Varnica, and P. Whiting, "Incremental redundancy hybrid ARQ with LDPC and raptor code," *IEEE Trans. Inf. Theory*, submitted, Sept. 2005.

[9] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–138, Oct. 1975.

[10] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[11] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, Mar. 2008, to appear.

[12] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, July 2006, pp. 957–961.

[13] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel with collective secrecy constraints," in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, July 2006, pp. 1164–1168.

[14] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, Jun. 2008, to appear.

[15] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, Jul. 2006, pp. 356–360.

[16] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, Jun. 2008, to appear.

[17] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of indepedent parallel channels," in *Proc. 44th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, Sep. 2006.

[18] P. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, submitted, Oct. 2006. [Online]. Available: http://arxiv.org/abs/cs/0610103

[19] S. Shamai (Shitz), L. Ozarow, and A. Wyner, "Information theoretic considerations for cellular mobile radio," *IEEE Trans. Veh. Technol.*, vol. 43, no. 2, pp. 359–378, May 1994.

[20] E. Biglieri, J. Proakis, and S. Shamai (Shitz), "Fading channels: Information-theoretic and communications aspects," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 1895–1911, Oct. 1998.

[21] H. Holma and A. Toskala, *WCDMA for UMTS*, 2nd ed. New York: Wiley, 2002.

[22] T. Cover and J. Thomas, *Elements of Information Theory*. New York: John Wiley & Sons, Inc., 1991.

[23] M. Zorzi and R. R. Rao, "On the use of renewal theory in the analysis of ARQ protocols," *IEEE Trans. Commun.*, vol. 44, no. 9, pp. 1077–1081, Sep. 1996.

[24] *Physical Layer Standard for CDMA2000 Spread Spectrum Systems (Revision C)*, 3GPP2 Std. C.S0002-C, 2004.

[25] J. Luo, R. Yates, and P. Spasojevic, "Service outage based power and rate allocation for parallel fading channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2594–2611, Jul. 2005.

[26] T. Ghanim and M. Valenti, "The throughput of hybrid-ARQ in block fading under modulation constraints," in *Proc. IEEE Conference on Information Sciences and Systems*, Princeton, NJ, Mar. 2006.

[27] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell Syst. Tech. J.*, vol. 63, no. 10, pp. 2135–2157, Dec. 1984.

[28] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. McLaughlin, and J. M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[29] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevic, "Secure nested codes for type II wiretap channels," in *Proc. IEEE Information Theory Workshop on Frontiers in Coding Theory*, Lake Tahoe, CA, Sep. 2-6, 2007.